Concurrency and Computation: Practice and Experience

Special Issue on Trust Management in Internet of Things

Scope
The Internet of Things (IoT) industry is booming in 2017, and the number of connected devices in use worldwide is expected to reach 8.4 billion, according to a recent Gartner report. It predicts that more than 20.8 billion IoT devices will be in use by 2020. However, due to the open nature of Internet connectivity, there are many challenges for IoT environments. For example, IoT is in no way immune to hacking. Attackers can launch DDoS attacks by infiltrating and leveraging thousands or millions of unsecured devices. In addition, most the embedded firmware running on IoT devices is insecure and highly vulnerable, leaving an indeterminate number of critical systems and data around the world at risk. As connected homes, cars, and offices become more mainstream, there is a significant need to develop more secure and trusted IoT environments.

This special issue focuses on how to build trust and hold effective trust management in an IoT environment, and identifies new issues and directions for future research and development work. We aim to solicit original research papers that discuss novel ways in trust management for IoT devices. Some good papers from IFIPTM 2019 will be invited to submit an extended version to this special issue.

Topics of interest:
We encourage the submission of high-quality contributions regarding the recent advances in IoT trust management. Topics of interest include, but are not limited to the ones listed below.

- Trust in Information Technology
- Formal aspects (specification, reasoning, and analysis)
- Trust-based and trust-aware IT policy management
- Trust in social networks and emerging contexts
- Trust in collaborative applications, crowd-sourcing and wiki systems
- Trust in human-computer interaction and usable systems
- Metrics and computation
- Socio-Technical and Sociological Trust
- Economic modeling of trust, risk and control; economics of trusted data quality
- Trust, control and reputation effects in social networking, e- and m-commerce
• Trust and socio materiality; socio-technical network structures; biological trust
• Ethical, sociological, psychological, legal aspects
• Trust and Identity Management
• Architectures and models
• Benchmarks, metrics and computation
• Anonymity, privacy and accountability
• Identity and personal information brokering
• Legal aspects
• Platforms and standards
• Blockchain and its use in trust
• Edge Computing in trust
• Big data technology in trust
• Self-explaining systems
• Trust in Cloud environments

Important Dates:
Submission deadline: September 15, 2019
Initial notification: November 30, 2019
Final Acceptance/rejection notification: February 1, 2020

Submission Guidelines:
Authors should prepare their manuscript according to the guide for authors available from the online submission page at http://www.cc-pe.net/journalinfo/authors.html.

Authors should select “SI: IoT Trust” when they reach the “Article Type” step in the submission process. Submitted papers must contain original work, which has neither been previously published nor it is currently under review by another journal or conference. Previously published or accepted conference papers must contain at least 40% new material to be considered for the special issue.

All papers will be peer-reviewed by at least three independent reviewers. Requests for additional information should be addressed to the corresponding guest editor.
Guest Editors:

Dr. Weizhi Meng (leading)
Technical University of Denmark, Denmark
E-mail: weme@dtu.dk

Dr. Christian D. Jensen
Technical University of Denmark, Denmark
E-mail: cjde@dtu.dk

Prof. Piotr Cofta
University of Science and Technology (UTP), Poland
Email: piotr.cofta@utp.edu.pl

Dr. Tyrone W A Grandison
Data-Driven institute, USA
Email: tgrandison@gmail.com

Editor Biography:

Dr. Weizhi Meng is currently an assistant professor in the Cyber Security Section, Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Denmark. He obtained his Ph.D. degree in Computer Science from the City University of Hong Kong (CityU), Hong Kong. Prior to joining DTU, he worked as a research scientist in Infocomm Security (ICS) Department, Institute for Infocomm Research, A*Star, Singapore, and as a senior research associate in CS Department, CityU. He won the Outstanding Academic Performance Award during his doctoral study, and is a recipient of the Hong Kong Institution of Engineers (HKIE) Outstanding Paper Award for Young Engineers/Researchers in both 2014 and 2017. He is also a recipient of Best Paper Award from ISPEC 2018, and Best Student Paper Award from NSS 2016. His primary research interests are cyber security and intelligent technology in security, including intrusion detection, smartphone security, biometric authentication, HCI security, trust computing, blockchain in security, and malware analysis. He served as program committee members for 20+ international conferences. He has been or will be a co-PC chair for IEEE Blockchain 2018, IEEE ATC 2019, IFIPTM 2019, Socialsec 2019. He also served as guest editor for FGCS, JISA, Sensors, CAEE, IJDSN, SCN, WCNC, etc.
Dr. Christian D. Jensen is now Associate Professor and Head of Cyber Security Section, at DTU Computer, Technical University of Denmark. He is coordinating the Specialist Programme in Cyber Security, which has been defined in collaboration with industry and government agencies to meet the increasing demand for graduates in computer security. His current research focuses on security in ubiquitous computing, particularly on the development of models, policies and mechanisms to support secure collaboration in open dynamic systems, such as pervasive computing environments, sensor networks and the Internet of Things (IoT). He is particularly interested in the problem of securing interactions between parties who do not necessarily share a common security infrastructure, e.g., sharing resources and information in open smart environments, across multiple organizations or across the Internet. He has been 20 years in this area of security and trust, and is widely recognized as one of the world’s leading experts in the area of computational trust and trust management, which focus on decentralized decision making under incomplete knowledge, biased in formation and potentially conflicting interests among agents in the system.

Prof. Piotr Cofta is a Professor in Computer Science at the University of Science and Technology (UTP) in Bydgoszcz, Poland. His long-term interest is in technology and trust, specifically computational forms of trust. He is a thought leader in system design methodology for secure and trustworthy information systems. He has almost 40 years of experience. He graduated (1980) and subsequently received PhD (1989) from the Technical University of Gdansk, Poland. He received his habilitation (2015) from the PJATK Warsaw, Poland. His interest currently focuses on novel forms of trust assurance, such as blockchains. His experience spans both the academia and the industry. Prior to the UTP he was (among others) a Chief Architect and a CTO in start-ups involved in trusted resource management, Chief Researcher in British Telecom investigating trust and security, Principal Investigator in MIT Media Lab Europe running the Trusting Technologies research group, Principal Scientist in Nokia investigating trust and mobile commerce etc. He has authored about 70 papers on the subject of trust and technology, including three books. He is also an inventor or co-inventor of more than 10 granted patents from the area of trust management. He is a Senior Member of the IEEE.

Dr. Tyrone W A Grandison is the Executive Director of The Data-Driven institute, which is a public health non-profit that helps policymakers create and implement effective programs and policies to solve their most critical problems, using the knowledge of the community, data and technology. He received a Ph.D. degree in Computer Science from the Imperial College of Science, Technology & Medicine in London (2003). Dr. Grandison has over 25 years experience in software engineering, security and privacy. His work in database security and privacy has been internationally recognized as pioneering and impactful. In addition to relational data privacy and security, he has created and successfully led research and product initiatives in RFID data management, privacy-preserving mobile data management, private social network analysis, text analytics and healthcare management systems.

He is also a 2018 Zhi-Xing Eisenhower Fellow. Dr. Grandison was the first-ever Chief Information Officer (CIO) of the Institute of Health Metrics and Evaluation at the University of Washington.
He also advises the Government of Jamaica on their Information Technology strategy - as a member of the National Information and Communications Technology Advisory Council (2016-18). He was the Deputy Chief Data Officer (dCDO) at the US Department of Commerce (2015-16), where he co-founded the Commerce Data Service - a data startup within the Department that supported its twelve bureaus - and led the successful rollout of its first 15 products. He was also a White House Presidential Innovation Fellow (2014-15) working with the US Department of Labor and the US CENSUS Bureau on their data and API (application programming interface) initiatives. He was the CEO of Proficiency Labs International, which specializes in supporting organizations design, build and evaluate privacy and security solutions for their systems. He co-founded woyhd.org, a service to help consumers determine the privacy awareness of mobile healthcare apps. He is the co-founder of Hipaantrepreneurs, a service to help healthcare professionals with compliance with healthcare law. He was one of the founding chairs of the Diversity in Privacy and Security Seminar (Di-PaSS) series, which seeks to increase the number of minority professionals and researchers in the privacy and security space. He is a founding partner of Wonder Women Hacks, which is a hackathon dedicated to increasing the number of women in tech, providing a support system for female technologists and helping to solve issues relevant to women. He is a founding partner of Hacks for Humanity (a collaboration with Arizona State University’s Project Humanities), which seeks to develop technology to reconnect people to their humanity. He is also an Adjunct Professor at the University of Technology in Kingston, Jamaica. Dr. Grandison was the CTO/co-founder of EqualityTV, where he led the platform and technical strategy initiatives.